Chapter 3
Cybersecurity, Purchasing Cards, and Follow-up on Prior Year Observations

Key Messages

- The Province continues to develop its cybersecurity risk management program
- Government organizations are not assessing the risks related to the use of purchasing cards
- Government organizations have taken some actions, yet are not managing fraud risks quickly enough
- The Province, the NSTU, and the Trustee are looking for ways to improve the long-term financial health of the Nova Scotia Teachers' Pension Plan
- Government has not yet provided promised guidance on internal meetings and employee social events costs

Details Around Key Messages

The Province's cybersecurity risk management program continues to develop

Observation	Example
In 2016, the Province initiated a cybersecurity program	• Created a Cyber Security and Risk Management Division • Hired a Chief Information Security Officer in 2016 • Adopted recognized frameworks to address cybersecurity risks • Shared Services regulations are not yet finalized
The Department of Service Nova Scotia and Internal Services may not be managing all of its cybersecurity risks	• The Cyber Security Risk Management Division manages its own risks, but the government-wide risk register is still in development
Survey results of 10 government organizations show a varied understanding of cybersecurity responsibilities	• 2 organizations noted they are not responsible for cybersecurity, yet they do in fact have responsibilities • 3 organizations noted they do not have a cybersecurity governance structure • 4 organizations noted they do not have a cybersecurity risk management program, which is concerning

Half of surveyed government organizations have not assessed purchasing card risks

Observation	Example
1 of 8 surveyed organizations using purchasing cards has not implemented a purchasing card policy	• Nova Scotia Municipal Finance Corporation
4 of 8 government organizations have not assessed the risks of using purchasing cards	• Halifax Regional Centre for Education • Nova Scotia Farm Loan Board • Nova Scotia Liquor Corporation • Nova Scotia Municipal Finance Corporation

Government departments and organizations are not managing fraud risks quickly enough

Observation	Example
Overall, too many fraud risk assessments are not completed, leaving uncertainty over fraud risk	• 47% of government departments have not completed fraud risk assessments • Department of Service Nova Scotia and Internal Services has significant control weaknesses and has not completed a fraud risk assessment • 43% of government organizations have not completed fraud risk assessments
Slow progress in implementing fraud risk management programs in the education sector	• Six educational organizations have no fraud policy and have not completed fraud risk assessments • The Department of Education and Early Childhood Development has not completed a fraud risk assessment
Mandatory fraud training is not being taken as required	• Less than 35% of staff completed mandatory fraud training at 3 government departments and 4 public service units
Slow progress in evaluating the use of a fraud tip hotline, the most effective method of discovering fraud	• 25% of government organizations still have not evaluated the need for a fraud tip hotline

Questions Nova Scotians may want to ask:

1. What is being done to ensure cybersecurity risks throughout the Province's IT environment are fully managed?
2. Why are there organizations that do not understand their cybersecurity responsibilities and what will be done about this?
3. What is the plan for finalizing the Shared Services regulations to list the government organizations that are to use the Province's IT services?
4. Why is it taking so long for a government that collects nearly $12 billion a year to have its fraud risks fully assessed and employees complete mandatory fraud training?
5. Why are fraud management programs nearly non-existent in regional centres for education which have had internal control weaknesses present for many years?
6. When will the Province's fraud reporting service/ hotline be available?
7. How does the Government create awareness of its fraud management program with its employees and the public?
8. How are government organizations ensuring adequate controls are in place relating to purchasing card spending if risk assessments are not completed?
9. Will the findings of the consultant's report on the teachers' pension plan be used to improve the financial health of the plan?

3 Cybersecurity, Purchasing Cards, and Follow-up on Prior Year Observations

Purpose

3.1 The purpose of this chapter is to inform Nova Scotians on important selected matters potentially impacting the Province. This chapter addresses cybersecurity, government purchasing cards, and follows up on previously reported matters in the areas of fraud risk management, public sector pensions, and internal meetings and employee social events expenses.

3.2 In following up on matters from our October 2018 Financial Report, we inquired of management at government departments, public service units, and organizations and reviewed information on their websites. These areas noted above, as well as management's responses, have not been audited; however, we did confirm the contents of this chapter with the named organizations.

Cybersecurity

3.3 Background – As with any organization, cybersecurity is a significant risk facing the Province. It is critical for government departments and organizations to understand and effectively manage cybersecurity risks.

3.4 In 2016, the Department of Service Nova Scotia and Internal Services (SNS-IS)[1] hired a Chief Information Security Officer to develop a cybersecurity program and lead a Cyber Security and Risk Management Division (Division), reporting directly to the Associate Deputy Minister.

3.5 SNS-IS management indicated that the Cyber Security and Risk Management Division is responsible for the security of the Province's network used by approximately 70 government organizations. Efforts to protect the network include:

- identifying cybersecurity risks to the Province
- approving new technology or changes to existing technology to ensure it is secure
- managing the Province's anti-virus software and firewalls
- performing vulnerability scans on the network and conducting penetration testing
- notifying other departments or divisions when risks that impact their information technology are identified

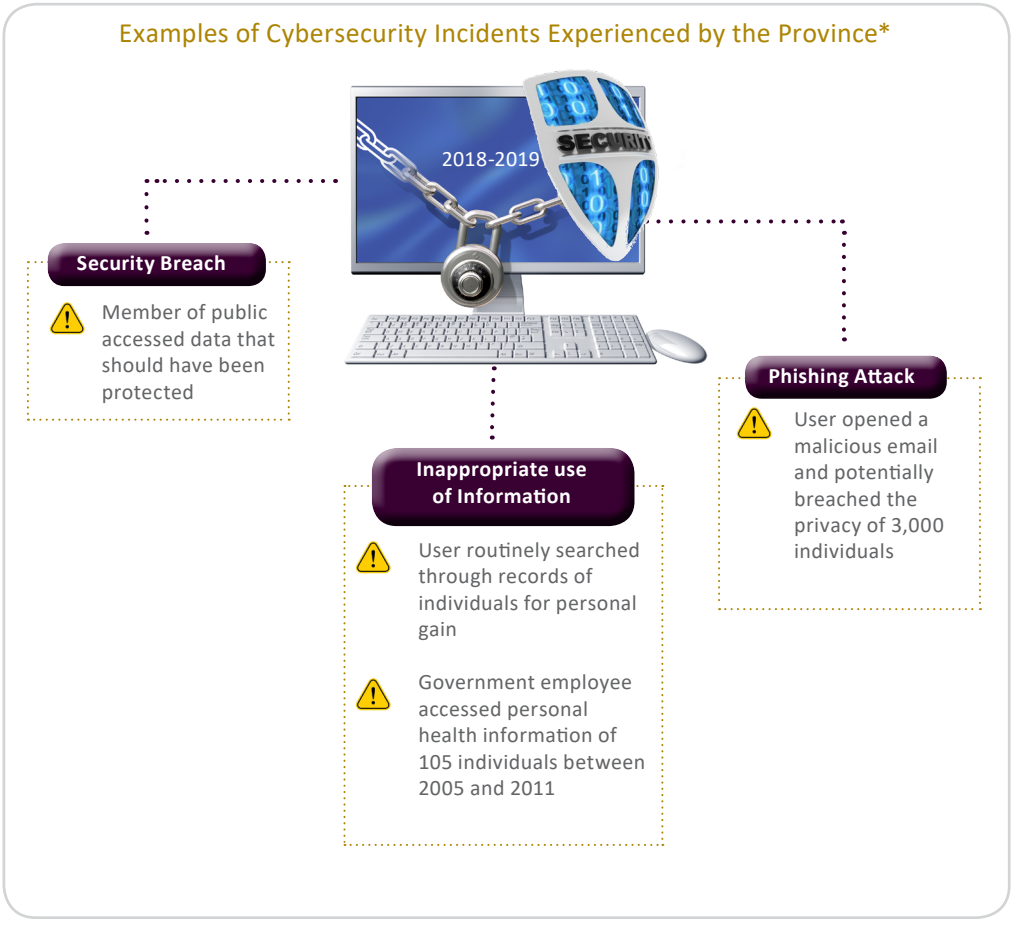
[1] *The Department of Internal Services was renamed the Department of Service Nova Scotia and Internal Services on June 3, 2019*

- implementing a mandatory cybersecurity awareness and education program for all employees (in progress)

3.6 Threats to an organization's cybersecurity can be from external hackers, business partners, vendors, contractors, or employees who either intentionally or unintentionally compromise cybersecurity. Cybercriminals, or trusted employees and partners, can affect the confidentiality, integrity, and availability of government's information technology or data, whether managed in-house or through cloud services. Impacts to the Province could include:

- information held for ransom
- theft of financial assets
- misuse of personal or financial information
- disruption of operations

3.7 The following diagram details some of the Province's recent cybersecurity incidents reported by the media.



** Details of these specific cybersecurity incidents were obtained from local media reporting.*

Regulations requiring organizations to obtain IT shared services have not been finalized

3.8 The Shared Services Act of 2014 requires that regulations be developed to define what shared services are to be provided and what departments, crown corporations, and government organizations are to receive those shared services. These regulations have not been finalized; however, management indicated they are currently being drafted. Finalizing these regulations would assist organizations in understanding their responsibilities for addressing cybersecurity risks.

The Province initiated a cybersecurity risk management program

3.9 The Province continues to develop its cybersecurity risk management program. The program uses guidance and objectives from the NIST Cyber Security framework and the Canadian Centre for Cybersecurity, which are industry accepted standards. SNS-IS created a charter for the Province's Cyber Security and Risk Management Division that outlines the principles to be followed by organizations under the Shared Services Act.

The Department of Service Nova Scotia and Internal Services may not be managing all of its cybersecurity risks

3.10 As part of a cybersecurity risk management program, an organization should establish a process for identifying, assessing, and managing all cybersecurity risks. SNS-IS indicated that the Cyber Security and Risk Management Division maintains its own risk register; however, SNS-IS is still developing a government-wide IT risk management program that will consider all components of cybersecurity, not just those areas under the Division's responsibility. As a result, at present, SNS-IS may not be managing all of its cybersecurity risks faced by the Province.

3.11 We encourage the Department of Service Nova Scotia and Internal Services to maintain its risk registers and to implement their government-wide IT risk management program in a timely manner.

Cybersecurity is a shared responsibility

3.12 Although IT services were centralized and the Cyber Security and Risk Management Division was created, government departments and organizations still have some level of responsibility for cybersecurity. For example, government organizations can have cybersecurity responsibility for their data, information technology (e.g., applications, databases, servers), medical technology (e.g., heart monitors, drug dispensing equipment) or technology capable of connecting to the internet (e.g., cell phones, tablets, watches). The level of responsibility is dependent on each organization's IT environment.

Next
Back
Prior View

3.13 Some government organizations use the Province's data centre and network to run their own applications and store data. Other government organizations operate applications and store data independently on their own networks or in the cloud. Regardless, all government organizations that own data, applications, servers, or manage networks have certain responsibilities and roles in relation to cybersecurity.

3.14 The size, complexity, and constant evolution of government operations require that organizations understand their cybersecurity responsibilities. We surveyed 10 significant government organizations to determine their perspective on cybersecurity responsibilities, whether they have governance structures in place to deal with cybersecurity, and if they implemented a cybersecurity risk management program.

Responses from Government Organizations on Cybersecurity

Government Organization	Level of Responsibility for Cybersecurity	Cybersecurity Governance Structure in Place	Cybersecurity Risk Management Program Implemented
Halifax-Dartmouth Bridge Commission	Shared	Yes	No
Halifax Regional Centre for Education	Full	Yes	Yes
Housing Nova Scotia	None	No	No
Izaak Walton Killam Health Centre	Shared	Yes	Yes
Nova Scotia Community College	Full	Yes	Yes
Nova Scotia Farm Loan Board	Shared	Yes	No
Nova Scotia Health Authority	None	No	Yes*
Nova Scotia Legal Aid Commission	Shared	Yes	Yes
Nova Scotia Liquor Corporation	Shared	Yes	Yes
Nova Scotia Municipal Finance Corporation	Shared	No	No
Total	**2 Full 6 Shared 2 None**	**7 Yes (70%) 3 No (30%)**	**6 Yes (60%) 4 No (40%)**

** Nova Scotia Health Authority indicated in their survey response that they rely extensively on SNS-IS for cybersecurity services and therefore has in place a cybersecurity risk management program. (unaudited)*

Results of the survey show a varied understanding of cybersecurity responsibilities

3.15 Because all organizations surveyed own applications or data, it would be expected that all would have some level of responsibility for cybersecurity. Eight of the 10 organizations surveyed indicated they have either shared or full responsibility for the cybersecurity of their information technology.

3.16 Nova Scotia Health Authority indicated in its survey response that it relies extensively on SNS-IS for cybersecurity services and therefore does not have cybersecurity responsibilities for IT infrastructure. However, the Health

Authority has cybersecurity responsibilities for many clinical applications and related data which are not managed by SNS-IS. As part of the annual financial statement audit of the Health Authority, we recommended that it define the scope of its cybersecurity responsibilities and implement a cybersecurity program. Management agreed with the recommendation.

3.17 In its survey response, Housing Nova Scotia identified that SNS-IS was fully responsible for its cybersecurity as a result of its relationship to the Department of Municipal Affairs and Housing (previously Department of Community Services). However, Housing Nova Scotia uses a system supported by a third-party vendor and therefore has cybersecurity responsibilities.

3 government organizations surveyed indicated they do not have a cybersecurity governance structure

3.18 Organizations should have a governance structure in place to ensure roles and responsibilities are known and understood. Housing Nova Scotia, Nova Scotia Health Authority, and Nova Scotia Municipal Finance Corporation commented that they rely on SNS-IS for their cybersecurity services and therefore do not have a cybersecurity governance structure. Without such structure, confusion about roles and responsibilities for specific aspects of cybersecurity is possible and creates opportunities for security weaknesses.

4 government organizations surveyed reported they do not have a cybersecurity risk management program

3.19 A cybersecurity risk management program provides definitive information on how an organization will manage cybersecurity-related risks. Survey results show that as at March 31, 2019, four organizations surveyed had not implemented a program.

- Halifax-Dartmouth Bridge Commission indicated they are in the development stage
- Housing Nova Scotia, Nova Scotia Farm Loan Board, and Nova Scotia Municipal Finance Corporation indicated they rely on SNS-IS

3.20 The Nova Scotia Health Authority indicated that it depends on SNS-IS for cybersecurity and as a result, relies on SNS-IS to manage the Health Authority's cybersecurity risks around IT infrastructure. Consequently, the Health Authority reported it has a cybersecurity risk management program; however, SNS-IS's risk frameworks do not take into consideration the Nova Scotia Health Authority's clinical data and applications. The Health Authority indicated it has started to plan a cybersecurity strategy in consultation and collaboration with SNS-IS.

Next
Back
Prior View

3.21 Reliance on SNS-IS for IT services is valid; however, this does not alter an organization's responsibility to implement its own cybersecurity risk management program appropriate to its IT environment. An organization must ensure that any data or applications for which it is responsible are protected against cybersecurity risks.

Purchasing Card Risk Management

3.22 Background – Purchasing cards are credit cards that are paid directly by the employer without the cardholder having to initially provide purchasing support. As a result, it is important for an organization to demonstrate strong oversight in this area by:

- implementing a thorough purchasing card policy
- assessing fraud risks over purchasing cards
- monitoring and reporting on purchasing card controls

3.23 We inquired of 10 of the Province's significant organizations about their use of purchasing cards. We asked if they used purchasing cards, and if so, did they have a purchasing card policy in place and if they had formally assessed the risks and key controls pertaining to purchasing cards.

3.24 Both Housing Nova Scotia and the Nova Scotia Legal Aid Commission confirmed that they do not use purchasing cards. The responses from the eight organizations that use purchasing cards are summarized below.

Responses from Government Organizations on Purchasing Cards

Government Organization	Purchasing Card Policy Implemented	Purchasing Card Risk and Control Assessments Completed
Halifax Regional Centre for Education	Yes	No
Halifax-Dartmouth Bridge Commission	Yes	Yes
Izaak Walton Killam Health Centre	Yes	Yes
Nova Scotia Community College	Yes	Yes
Nova Scotia Farm Loan Board	Yes	No
Nova Scotia Health Authority	Yes	Yes
Nova Scotia Liquor Corporation	Yes	No
Nova Scotia Municipal Finance Corporation	No	No
Total	**7 Yes (88%) 1 No (12%)**	**4 Yes (50%) 4 No (50%)**

Next
Back
Prior View

1 significant organization surveyed has not implemented a purchasing card policy

3.25 Our survey shows that the Nova Scotia Municipal Finance Corporation is the only surveyed government organization using purchasing cards that has not yet implemented a purchasing card policy. It is important that the Nova Scotia Municipal Finance Corporation implement a purchasing card policy to assist in holding cardholders accountable and ensure that purchasing card transactions are appropriately reviewed, approved, and recorded.

4 of 8 surveyed government organizations using purchasing cards have not assessed the risks related to their use

3.26 Our survey also shows the need for government organizations that use purchasing cards to assess the risks relating to their use and ensure that adequate controls are in place to manage the risk of fraud. The following four surveyed organizations using purchasing cards confirmed that they have not completed a formal risk or control assessment related to purchasing cards.

- Halifax Regional Centre for Education
- Nova Scotia Farm Loan Board
- Nova Scotia Liquor Corporation
- Nova Scotia Municipal Finance Corporation

3.27 While the use of purchasing cards may be an effective way to purchase goods or services, without assessing the risks relating to purchasing card spending, it is difficult for government organizations to ensure adequate controls are in place relating to their use.

Update on Fraud Risk Management

3.28 Background – Fraud within the public sector is concerning because it can result in the loss of taxpayer assets and reduce the public's confidence in the Province's financial reporting. It is important for the Province to have mechanisms in place to appropriately manage fraud risk.

3.29 To manage fraud risk, the Province, in 2017 implemented a fraud policy. The policy directly applies to all government departments, public service units, and crown corporations, and although not required, it was recommended that other government organizations embrace the intent of the policy. A Fraud Management Committee governs the departmental fraud risk management program. Specific components of the program include:

- Fraud policies and procedures
- Fraud risk assessments

- Fraud awareness and education
- Fraud prevention and detection techniques

3.30 In 2017, we identified weaknesses in the Province's fraud risk management program and recommended that Executive Council Office ensure those responsible for oversight of government departments and organizations address these weaknesses. Last year, we followed up and noted that government departments and organizations were slow in improving their management of fraud risks.

Fraud risk management programs are not improving quickly enough

3.31 2019 follow-up – We followed up with Executive Council Office for an update on the status of the fraud risk management program. See Appendix V for the update from the Chair of the Deputy Ministers' Audit Committee on the Government's fraud management program.

3.32 We also followed up with government departments and organizations for updates on the status of their fraud risk management programs. The table below summarizes the status as at March 31, 2019 and Appendices I and III show the status of each individual department and organization.

Summary Status of Certain Aspects of Fraud Risk Management Programs in Government Departments and Organizations

	March 31, 2019	March 31, 2018
Government Departments		
Fraud risk assessment	9 Yes (53%) 8 No (47%)	3 Yes (18%) 14 No (82%)
Government Organizations		
Fraud policy	42 Yes (82%) 9 No (18%)	33 Yes (65%) 18 No (35%)
Fraud risk assessment	29 Yes (57%) 22 No (43%)	10 Yes (20%) 41 No (80%)
Evaluated usefulness of fraud hotline	38 Yes (75%) 13 No (25%)	23 Yes (45%) 28 No (55%)

47% of government departments have not completed fraud risk assessments

3.33 As at March 31, 2019, 8 of 17 (47%) departments had not completed fraud risk assessments. This may be an improvement from last year; however, progress is not fast enough.

3.34 Many sizeable departments, such as Education and Early Childhood Development, and Internal Services[2], still have not completed fraud risk

[2]*The Department of Internal Services was renamed the Department of Service Nova Scotia and Internal Services on June 3, 2019*

Next
Back
Prior View

assessments. All departments should complete fraud risk assessments; however, the need for the Department of Service Nova Scotia and Internal Services to complete its assessment is elevated because of the Department's significant control weaknesses.

57% of government organizations completed fraud risk assessments

3.35 Our 2019 follow-up of government organizations noted improvement in the number of fraud risk assessments completed. As at March 31, 2019, 57 percent of government organizations completed fraud risk assessments. This is an improvement from last year when 20 percent of organizations had completed fraud risk assessments.

6 public educational organizations do not have a fraud policy and have not completed a fraud risk assessment

3.36 The need for the seven regional centres for education and Conseil scolaire acadien provincial to effectively manage their fraud risks is important. However, the following do not have a fraud policy and have not yet completed a fraud risk assessment.

- Annapolis Valley
- Cape Breton-Victoria
- Chignecto-Central
- Conseil scolaire acadien provincial
- South Shore
- Tri-County

3.37 Department of Education and Early Childhood Development management indicated it plans to have each regional centre for education and Conseil scolaire acadien provincial complete a fraud risk assessment and implement a common fraud policy in 2019-20.

Province's fraud tip hotline not yet implemented

3.38 Fraud research conducted by the Association of Certified Fraud Examiners shows that tips are the most common method of detecting fraud[3]. In 2017, we noted that no government department was using a fraud tip hotline and recommended that the Province address this weakness. In 2017, the Province confirmed they would evaluate the usefulness of a fraud tip hotline and in 2018 expected to have it in place by December 2018. The Province has yet to implement a fraud tip hotline.

3.39 Government organizations should also evaluate the usefulness of a fraud tip hotline. Our enquiry of government organizations revealed that while 38 (75%) evaluated the usefulness of a fraud tip hotline, 13 (25%) did not. Refer to Appendix III for the status of each government organization.

[3] *Report to the Nations on Occupational Fraud and Abuse – 2014 Global Fraud Study, Association of Certified Fraud Examiners*

13 government departments and 4 organizations are not evaluating and reporting on the effectiveness of their fraud risk management programs

3.40 Regularly evaluating and reporting on fraud risk management operations helps a department or organization ensure it has designed an appropriate process that prevents and detects fraud in the current environment. Therefore, government departments and organizations should regularly evaluate and report on how well it is managing its fraud risks.

3.41 We surveyed all government departments and nine significant government organizations to determine if they regularly evaluate and report on whether their fraud risk management process is working effectively. The results are summarized in the table below and the status for each government department and organization is shown in Appendix I and IV, respectively.

Summary Status of Government Departments and Organizations Regularly Evaluating and Reporting on Effectiveness of Fraud Management

	Regularly Evaluate and Report on Effectiveness of Fraud Management
Government Departments	4 Yes (24%) 13 No (76%)
Government Organizations	5 Yes (56%) 4 No (44%)

Mandatory fraud training is not being taken as required

3.42 The Province's mandatory fraud training for government departments and public service units became available following release of the Government's Fraud Policy in June 2017 and helps in the management of fraud. Management's responses in Appendices I and II show fraud training completion rates range from 11 percent to 100 percent as at March 31, 2019. Low completion rates of mandatory fraud training diminish the Province's ability to effectively manage fraud.

3.43 The following table notes the three government departments and four public service units with fraud training completion rates below 35 percent.

Next
Back
Prior View

Departments and Public Service Units with Fraud Training Completion Rates Below 35%	
Department	**% of Employees who Completed Fraud Training as at March 31, 2019**
Transportation and Infrastructure Renewal	11%
Seniors	20%
Environment	31%
Public Service Unit	**% of Employees who Completed Fraud Training as at March 31, 2019**
Office of the Information and Privacy Commissioner	14%
Human Rights Commission	17%
Communications Nova Scotia	27%
Office of Regulatory Affairs and Service Effectiveness	27%

67% of significant government organizations surveyed provide fraud training

3.44 We surveyed nine significant government organizations to determine whether fraud training is provided. Although only three of nine organizations make fraud training mandatory, six of these organizations provide fraud training to employees. The survey results are summarized below.

Government Organization's Response to Fraud Training	
Government Organization	**Fraud Training Provided to all Employees**
Halifax-Dartmouth Bridge Commission	Yes
Halifax Regional Centre for Education	Yes
Izaak Walton Killam Health Centre	No
Nova Scotia Community College	No
Nova Scotia Farm Loan Board	Yes*
Nova Scotia Health Authority	No
Nova Scotia Legal Aid Commission	Yes
Nova Scotia Liquor Corporation	Yes*
Nova Scotia Municipal Finance Corporation	Yes*
Total	**6 Yes (67%)** **3 No (33%)**

** Management indicated fraud training is mandatory*

3.45 Employees who complete fraud training are better able to understand, prevent, and detect fraud and enhance an organization's ability to manage fraud. We encourage government organizations to evaluate the need for mandatory fraud training.

Update on Public Sector Pensions

3.46 Pension plans are a significant financial and legal liability of the Province of Nova Scotia and are important to public sector employees that plan on

receiving pension plans once they retire. In 2017, we highlighted the financial health of the three largest public sector pension plans in Nova Scotia – the health care plan, the public service plan, and the teachers' plan.

The Province, the Nova Scotia Teachers' Union, and the Trustee are looking at ways to improve the long-term financial health of the teachers' pension plan

3.47 In 2018, we followed up and found that the Province and the Nova Scotia Teachers' Union (the NSTU) did not have a formal plan in place to address the $1.4 billion deficit in the teachers' pension plan. We recommended the Province initiate discussions with the NSTU to develop and implement a formal plan to address the deficit.

3.48 During the year, the Province, the NSTU, and the Trustee, hired an independent pension consultant to identify ways to improve the long-term financial sustainability of the teachers' pension plan.

Update on Internal Meetings and Employee Social Events Expenses

Government has not yet provided promised guidance on internal meetings and employee social events costs

3.49 In 2018, we examined internal meetings and employee social events costs to determine if these expenses complied with existing policies, were appropriately supported, and correctly classified. From this work in 2018, we noted a lack of formalized policy across government in the areas of internal meetings and employee social events. We recommended that Executive Council provide guidance on internal meeting and employee social event expenses that clarifies the nature and accounting of acceptable costs to ensure these expenses meet public expectations, are supportable, and well-documented.

3.50 Guidance in this area would provide more direction to departments and employees. For example, an employee should be able to easily understand if costs for internal meetings or events such as birthdays, retirements, or Christmas parties are acceptable.

3.51 This year, we followed up with Executive Council Office to determine whether it provided guidance on internal meeting and employee social event expenses. We were informed that discussions on this matter are ongoing with a goal to establish corporate guidelines by the end of the calendar year and to implement the guidelines by January 1, 2020.

3.52 It is important that Executive Council Office address this recommendation, as there is a public expectation for these types of expenses to be well-managed.

Appendix I

Management's Responses from Government Departments Regarding Certain Aspects of a Fraud Management Program

Of the 17 government departments listed in Schedule 10 of the 2019 Public Accounts, below is the March 31, 2019 status of certain aspects of a fraud management program.

Government Department	Fraud Risk Assessment	Evaluate and Report on Effectiveness of Fraud Risk Management	% of Employees who Completed Fraud Training as at March 31, 2019
Agriculture	No	No	65%
Business	Yes	No	54%
Communities, Culture and Heritage	No*	No	48%
Community Services	Yes	No	38%
Education and Early Childhood Development	No	No	55%
Energy and Mines	Yes	Yes	62%
Environment	No	No	31%
Finance and Treasury Board	Yes	No	50%
Fisheries and Aquaculture	No	No	57%
Health and Wellness	Yes	No	63%
Internal Services[4]	No	No	65%
Justice	Yes	Yes	66%
Labour and Advanced Education	Yes	Yes	90%
Lands and Forestry	No	No	66%
Municipal Affairs[5]	No*	No	96%
Seniors	Yes	No	20%
Transportation and Infrastructure Renewal	Yes	Yes	11%
Total	**9 Yes (53%) 8 No (47%)**	**4 Yes (24%) 13 No (76%)**	**–**

**Management indicated progress is being made (unaudited)*

[4]*The Department of Internal Services was renamed the Department of Service Nova Scotia and Internal Services on June 3, 2019*
[5]*The Department of Municipal Affairs was renamed the Department of Municipal Affairs and Housing on June 3, 2019*

Appendix II

Management's Responses from Public Service Units Regarding Mandatory Fraud Training Completion Rates

Of the 18 public service units listed in Schedule 10 of the 2019 Public Accounts, below is the March 31, 2019 status of mandatory fraud training completion rates.

Public Service Unit	% of Employees who Completed Fraud Training as at March 31, 2019
Aboriginal Affairs	59%
Communications Nova Scotia	27%
Elections Nova Scotia	67%
Executive Council	76%
Human Rights Commission	17%
Intergovernmental Affairs	53%
Legislative Services	94%
Nova Scotia Police Complaints Commissioner	75%
Nova Scotia Securities Commission	38%
Office of Immigration	80%
Office of Regulatory Affairs and Service Effectiveness	27%
Office of Service Nova Scotia	60%
Office of Strategy Management	100%
Office of the Auditor General	97%
Office of the Information and Privacy Commissioner	14%
Office of the Ombudsman	88%
Public Prosecution Service	50%
Public Service Commission	97%

Next
Back
Prior View

Appendix III

Management's Responses from Government Organizations Regarding Certain Aspects of a Fraud Management Program

Of the 53 active government organizations (governmental units, government business enterprises, government partnership arrangements) listed in Schedule 10 of the 2019 Public Accounts, below is the March 31, 2019 status of certain aspects of a fraud management program.

Government Organization	Fraud Policy	Fraud Risk Assessment	Evaluated Usefulness of Fraud Hotline
A. Education Sector			
Annapolis Valley Regional Centre for Education	No	No	Yes
Atlantic Provinces Special Education Authority	No	No	No
Cape Breton-Victoria Regional Centre for Education	No	No	No
Chignecto-Central Regional Centre for Education	No	No	No
Education Conseil scolaire acadien provincial	No	No	No
Halifax Regional Centre for Education	Yes	No	Yes
Nova Scotia Education Common Services Bureau	No	No	No
Nova Scotia Community College	Yes	Yes	Yes
Nova Scotia School Insurance Exchange	Yes	No	No
Nova Scotia School Insurance Program Association	Yes	No	No
South Shore Regional Centre for Education	No	No	Yes
Strait Regional Centre for Education	No	Yes	Yes
Tri-County Regional Centre for Education	No	No	No
B. Health Sector			
Izaak Walton Killam Health Centre	Yes	Yes	Yes
Nova Scotia Health Authority	Yes	No[6]	Yes
Nova Scotia Health Research Foundation	Yes	Yes	No
C. Sizeable Organizations			
Art Gallery of Nova Scotia	Yes	No	Yes
Canada-Nova Scotia Offshore Petroleum Board	Yes	Yes	Yes
Develop Nova Scotia	Yes	Yes	No
Halifax Convention Centre Corporation	Yes	No	Yes
Halifax-Dartmouth Bridge Commission	Yes	Yes	Yes

[6]Nova Scotia Health Authority management indicated that a fraud risk assessment is completed for 75% of expenditures (payroll) with a plan developed to complete the remainder (unaudited)

Government Organization	Fraud Policy	Fraud Risk Assessment	Evaluated Usefulness of Fraud Hotline
C. Sizeable Organizations			
Harbourside Commercial Park Inc.	Yes	Yes	Yes
Highway 104 Western Alignment Corporation	Yes	Yes	Yes
Housing Nova Scotia	Yes	Yes	Yes
Nova Scotia Business Inc.	Yes	Yes	Yes
Nova Scotia Crop and Livestock Insurance Commission	Yes	Yes	Yes
Nova Scotia Farm Loan Board	Yes	No	Yes
Nova Scotia Fisheries and Aquaculture Loan Board	Yes	No	Yes
Nova Scotia Gaming Corporation	Yes	Yes	Yes
Nova Scotia Innovation Corporation	Yes	Yes	Yes
Nova Scotia Lands Inc.	Yes	Yes	Yes
Nova Scotia Legal Aid Commission	Yes	No	Yes
Nova Scotia Liquor Corporation	Yes	Yes	Yes
Nova Scotia Municipal Finance Corporation	Yes	Yes	Yes
Nova Scotia Power Finance Corporation	Yes	Yes	Yes
Nova Scotia Utility and Review Board	Yes	Yes	Yes
Public Archives of Nova Scotia	Yes	Yes	No
Tourism Nova Scotia	Yes	Yes	Yes
D. Others			
Arts Nova Scotia	Yes	No	No
Canadian Sport Centre Atlantic	Yes	No	No
Council of Atlantic Premiers	Yes	Yes	Yes
Creative Nova Scotia Leadership Council	No Response	No Response	No Response
Gambling Awareness Foundation of Nova Scotia	Yes	No[7]	Yes
Invest Nova Scotia Board	Yes	Yes	Yes
Law Reform Commission of Nova Scotia	Yes	Yes	Yes
Nova Scotia Primary Forest Products Marketing Board	No Response	No Response	No Response
Nova Scotia Strategic Opportunities Fund Incorporated	Yes	No	Yes
Perennia Food & Agriculture Incorporated	Yes	No	Yes
Resource Recovery Fund Board Inc.	Yes	Yes	Yes
Schooner Bluenose Foundation	Yes	Yes	Yes
Sherbrooke Restoration Commission	Yes	Yes	Yes
Sydney Steel Corporation	Yes	Yes	Yes
Sydney Utilities Limited	Yes	Yes	Yes
Total	**42 Yes (82%) 9 No (18%)**	**29 Yes (57%) 22 No (43%)**	**38 Yes (75%) 13 No (25%)**

[7]Gambling Awareness Foundation of Nova Scotia management indicated that a fraud risk assessment has been started and is expected to be completed early in 2019-20 (unaudited)

Appendix IV

Management's Responses from Nine of the Province's Significant Organizations Regarding Evaluating and Reporting on the Effectiveness of Its Fraud Risk Management

Of nine significant organizations listed in Schedule 10 of the 2019 Public Accounts, below is the March 31, 2019 status of the organization regularly evaluating and reporting on the effectiveness of fraud risk management.

Government Organization	Regularly Evaluate and Report on Effectiveness of Fraud Risk Management
Halifax-Dartmouth Bridge Commission	Yes
Halifax Regional Centre for Education	No
Izaak Walton Killam Health Centre	No
Nova Scotia Community College	Yes
Nova Scotia Farm Loan Board	Yes
Nova Scotia Health Authority	Yes
Nova Scotia Legal Aid Commission	No
Nova Scotia Liquor Corporation	Yes
Nova Scotia Municipal Finance Corporation	No
Total	**5 Yes (56%)** **4 No (44%)**

Next
Back
Prior View

Appendix V

Update from the Chair of the Deputy Ministers' Audit Committee on Government's Fraud Management Program

Government has a Fraud Management Program to manage the risk of fraud. The Program is governed by a Fraud Management Committee, with government-wide representation, and oversight from the Deputy Ministers' Audit Committee. A formal mandate for the Fraud Management Committee outlines its purpose, authority, responsibilities, and composition. The step-by-step implementation of this Program is an explicit demonstration of Government's commitment to a sustainable culture of respect, integrity, diversity, accountability and the public good.

A Fraud Policy was included in the Corporate Administrative Policy Manuals, Management Manual 200 in 2017. The Policy is supported by detailed procedures for reporting and investigating fraud. In addition, mandatory fraud awareness training has been available online for government employees since the Policy was released. This has been completed by more than 7,100 employees and the completion rates are reviewed by the departments every three months. The training was recently updated to be compatible with Government's new learning platform and includes accessibility features that were not available in the previous version. The revised training has been formatted for a broader audience.

Government is committed to the completion of fraud risk assessments to identify and assess the likelihood and significance of specific fraud schemes and risks, evaluate control activities, and implement action to address fraud risks. Fraud risk assessments are completed and in progress; however, the completion rates need to improve. Government is supporting this effort with the use of a fraud risk assessment framework to ensure that assessments meet an appropriate standard and are consistently applied, a fraud risk self-assessment toolkit distributed to the departments to assess and identify areas at a high risk for fraud, the development of a streamlined process for procuring fraud risk assessments from third party service providers, and the development of an experienced team of fraud investigators with experience completing fraud risk assessments.

An independent third-party vendor has been selected through a government procurement process to manage the Provincial Fraud Reporting Service (e.g. hotline, webform, email reporting). The service will be available 24 hours a day, 365 days per year.

Next
Back
Prior View